JOURNAL OF COMPUTER AND SYSTEM SCIENCES 26, 92–106 (1983)

Multiplicative Complexity and Algebraic Structure

DAVE RIFFELMACHER

Bell Laboratories, Holmdel, New Jersey 07733

Received March, 1980; revised July 3, 1982

The classical structure theory of an (associative unitary) algebra A over a field F is invoked to determine upper bounds on the (bilinear) multiplicative complexity $\pi(A)$ of A over F. The upper bound problem for matrix multiplication over a finite extension F of the rational numbers is related to the multiplicative complexity problem for a certain twisted polynomial algebra. For certain base fields F (including finite extensions of the rationals and the real and complex fields) the order of complexity of an F-algebra with all nilpotent ideals having square zero is shown to be bounded above by the complexity of multiplying matrices over F.

1. INTRODUCTION

Fiduccia and Zalcstein [8] have unified the various multiplication problems, such as the multiplication of matrices and polynomials or more generally the evaluation of bilinear forms, by considering all of them as instances of the multiplication problem for a finite dimensional linear algebra. In this article, we exploit the classical algebraic structure theory of an n-dimensional (associative unitary) algebra A over a field F to derive upper bounds on the (bilinear) multiplicative complexity $\pi(A)$ of A over F for certain classes of F-algebras.

The definition of the (bilinear) multiplicative complexity $\pi(A)$ of the F-algebra A is recalled in Section 2 as well as some of the known bounds on $\pi(A)$ for various algebras A. Section 3 provides a brief overview of the classical structure theory of a finite dimensional algebra over a field. In addition to setting notation, these sections (and especially the frequent references to the literature) are intended as an aid to the reader unfamiliar with either multiplicative complexity or structure theory.

The multiplicative complexity of a central simple algebra (a type of algebra which incudes matrix algebras, see Definition 3.3) over an algebraic number field (i.e., a finite extension of the rational numbers) is the topic of Section 4. We show (Theorem 4.2) that if A and B are n-dimensional central simple algebras over a number field, $4\pi(A) \geqslant \pi(B) \geqslant \frac{1}{4}\pi(A)$. Hence all central simple algebras of the same dimension over number fields have the same order of complexity. Since total matrix algebras satisfy the tensor product algebra isomorphism

$$M(r, F) \otimes_F M(s, F) \simeq M(rs, F)$$

for all positive integers r and s, an upper bound on the complexity of central simple

0022-0000/83/010092–15$03.00/0

algebras of dimension p^2 for a prime p would yield an upper bound on the complexity of central simple algebras over number fields. Therefore, we focus on these algebras to prove (Theorem 4.5) that if A is a p^2-dimensional central simple algebra over the number field F containing all pth roots of unity, then $4\pi(T) \geqslant \pi(A) \geqslant \frac{1}{4}\pi(T)$ for a certain twisted truncated polynomial algebra $T = (F, \gamma)$, where γ is a pth root of unity.

Fiduccia [9, 10] has produced examples of n-dimensional linear algebras with multiplicative complexity bounded below by $n^2/3$. The goal of Section 5 is to show that, over certain fields, algebras with multiplication which is that hard to compute must have a certain nasty structural property, namely, a nilpotent ideal of nilpotency index greater than two. Specifically, we establish (Theorem 5.5) that if F belongs to a certain class of perfect fields (including number fields and the real and complex numbers) and A is an n-dimensional F-algebra with all nilpotent ideals having square zero, then there is a constant k such that $\pi(A) \leqslant kn^{1.5}$. This bound of 1.5 is not necessarily tight since it arises from a loose upper bound on the multiplicative complexity of a central simple F-algebra.

Throughout this article, A is an n-dimensional (associative unitary) algebra (perhaps with additional structure) over the field F and linear dimension is denoted by $(A:F) = n$. We assume the reader is familiar with the fundamentals of linear algebra and ring theory. The notation $\pi(A) = O(n^\alpha)$ is used to mean there exists a constant k with $\pi(A) \leqslant kn^\alpha$.

2. Review of Multiplicative Complexity

In this section, we briefly recall the definition of the (bilinear) multiplicative complexity of an algebra. Several well-known bounds on the multiplicative complexity of various algebras are also listed. The interested reader is referred to [8] for a broad survey of the multiplicative complexity literature.

Let A be an algebra over the field F with F-basis $\{e_i\}_{i=0}^{n-1}$. Given arbitrary elements $\sum_{i=0}^{n-1} x_i e_i$ and $y = \sum_{i=0}^{n-1} y_i e_i$ in A, the (bilinear) multiplicative complexity problem is to compute

$$x \cdot y = \left(\sum_{i=0}^{n-1} x_i e_i\right)\left(\sum_{i=0}^{n-1} y_i e_i\right) \equiv \sum_{j=0}^{n-1} z_j e_j$$

by means of an algorithm γ which proceeds by computing t products

$$p_k = \left(\sum_{i=0}^{n-1} a_{ki} x_i\right)\left(\sum_{i=0}^{n-1} b_{ki} y_i\right), \qquad a_{ki}, b_{ki} \in F$$

such that for $0 \leqslant j \leqslant n-1$

$$z_j = \sum_{k=1}^{t} c_{jk} p_k \qquad \text{for some} \quad c_{jk} \in F.$$

DEFINITION 2.1. The multiplicative complexity of the F-algebra A, denoted $\pi_F(A)$, is the minimum value of t for any such algorithm γ. (If the base field is clear from the context, we write $\pi_F(A) = \pi(A)$.)

It may be shown that $\pi(A)$ is independent of the particular F-basis chosen for A and thus $\pi(A)$ is well defined. The remainder of this section is a short extract of some of the interesting bounds on $\pi(A)$ to be found in the literature.

THEOREM 2.1. *If A is an n-dimensional F-algebra,*

$$n \leqslant \pi(A) \leqslant 3n^2/4.$$

Proof. Since A has a unitary element, the lower bound follows from a theorem of Fiduccia and Zalcstein [8]. The upper bound is due to Howell [13]. ∎

THEOREM 2.2 [8, Theorem 8]. *If A is a degree n field extension of F and F has at least $2n-1$ elements,*

$$\pi(A) = 2n - 1. \quad ∎$$

A nonzero element a of A is called a zero divisor if there is a nonzero element b of A with $ab = 0$. The absence of zero divisors in an algebra leads to the lower bound:

THEOREM 2.3 [8, Theorem 6]. *If A is an n-dimensional F-algebra with no zero divisors, $\pi(A) \geqslant 2n - 1$.* ∎

Given a polynomial $f(x)$ in the F-algebra $F[x]$ of polynomials in the indeterminate x over the field F, let

$$f(x) = \prod_{i=1}^{k} \{f_i(x)\}^{m_i}$$

be its prime factorization. The quotient algebra

$$F_f = F[x]/\langle f(x)\rangle$$

of $F[x]$ modulo the ideal generated by $f(x)$ then splits (by the Chinese remainder theorem) into a finite Cartesian product

$$F_f \simeq \prod_{i=1}^{k} \{F[x]/\langle f_i^{m_i}(x)\rangle\}$$

with k components. Bini and Capovani have recently shown

THEOREM 2.4 [4]. *Let* $f(x) = \prod_{i=1}^{k} f_i^{m_i}(x)$ *be the prime factorization of* $f(x)$ *in* $F[x]$. *Then*

$$\pi(F[x]/\langle f(x)\rangle) = 2n - k,$$

if F *has at least* $\max_i\{2n_i - 1\}$ *elements.* ∎

For a positive integer m, we denote the F-algebra of all $m \times m$ matrices over F by $M(m, F)$. If A is an F-algebra, $M(m, A)$ denotes the F-algebra of all $m \times m$ matrices with entries from A. Note that $(M(m, F): F) = m^2$.

THEOREM 2.5 [14, 15]. $\pi(M(2, F)) = 7$. ∎

The quaternion algebra $\mathbb{D}(F)$ over F is the four-dimensional algebra generated by the elements 1, i, j, and k, where

$$i^2 = j^2 = k^2 = -1, \qquad ij = k, \qquad jk = i, \qquad ki = j.$$

THEOREM 2.6 [7, 11]. *Let* F *be a field of characteristic not* 2. *Then* $\pi(\mathbb{D}(F)) = 8$. ∎

3. REVIEW OF ALGEBRAIC STRUCTURE THEORY

This section provides an introductory overview of that portion of the structure theory of (finite-dimensional) algebras over a field which will be required in later sections of this article. Proofs of theorems are not provided but references to relevant literature are given. An excellent general reference on classical structure theory is the book by Herstein [12].

DEFINITION 3.1. The center of the F-algebra A, denoted $Z(A)$, is the set of all elements x of A such that $xa = ax$ for all a in A.

EXAMPLE 3.1. (a) If A is a commutative algebra, $Z(A) = A$.

(b) For any F-algebra A and positive integer m, $Z(M(m, A)) = Z(A)$.

DEFINITION 3.2. The F-algebra A is called simple if A has no two-sided ideals except $\{0\}$ and A.

THEOREM 3.1 [12, Theorem 2.1.5]. *If* A *is a simple* F*-algebra, the center* $Z(A)$ *of* A *is a finite field extension of* F.

EXAMPLE 3.2. (a) The Cartesian product $F \times F$ is not simple since, for example, $F \times \{0\}$ is a nontrivial two-sided ideal.

(b) Any division algebra (an algebra where every nonzero element has a multiplicative inverse) is simple.

(c) The matrix algebra $M(m, F)$ is simple.

DEFINITION 3.3. The F-algebra A is a central simple F-algebra (CSA) if A is a simple F-algebra with $Z(A) = F$.

EXAMPLE 3.3. (a) The complex number field $\mathbf{C}$ is a simple algebra over the real number field $\mathbb{R}$ but not a central simple $\mathbb{R}$-algebra.

(b) Matrix algebra $M(m, F)$ is a central simple F-algebra.

(c) The quaternion algebra $\mathbb{D}(\mathbb{R})$ over the real field $\mathbb{R}$ is a central simple $\mathbb{R}$-algebra.

DEFINITION 3.4. Two central simple F-algebras A and B are similar if there exist positive integers r and s with

$$M(r, A) \simeq M(s, B).$$

The notion of similarity is an equivalence relation on the class of central simple F-algebras. We denote the equivalence class of A by $[A]$. A multiplication may be defined on these equivalence classes by defining $[A] \times [B] = [A \otimes_F B]$ for central simple F-algebras A and B. With this multiplication, the collection of equivalence classes of central simple F-algebras forms a group $\mathrm{B}(F)$, called the Brauer group of F.

THEOREM 3.2 [12, Theorem 2.16]. *A is a simple F-algebra iff $A \simeq M(m, D)$ for some positive integer m and division F-algebra D.* ∎

DEFINITION 3.5. *Let L be a finite field extension of F. Then L is a separable extension of F if the minimum polynomial of any element of L has no multiple roots.*

THEOREM 3.3 [12, Theorems 4.2.2, 4.3.3]. *Here, A is a central simple F-algebra iff $A \simeq M(m, D)$ for a central division F-algebra D. Moreover, D has a maximum separable subfield L containing F such that $(D:F) = (D:L)(L:F) = (L:F)^2$ and $D \otimes_F L \simeq M(r, L)$ for some r. Then L is called a splitting field for D and A.* ∎

DEFINITION 3.6. If L is a finite separable extension field of F, the relative Brauer group $\mathrm{B}(L/F)$ is defined as the subgroup of $\mathrm{B}(F)$ generated by equivalence classes of algebras split by L.

DEFINITION 3.7. The finite extension L of F is a Galois extension of F if

$$F = \{x \in L \mid \sigma(x) = x \text{ for all } F\text{-linear automorphisms } \sigma \text{ of } L\}.$$

If L is Galois over F, the group of all F-linear automorphisms of L is called the Galois group of L over F, denoted $\mathrm{Aut}(L/F)$.

DEFINITION 3.8. Let L be a Galois extension of F with $G = \mathrm{Aut}(L/F)$. A function

$$f: G \times G \to L^* \equiv L - \{0\}$$

is called a factor set on G in L if, for all σ, τ, ρ in G,

$$f(\sigma, \tau\rho) f(\tau, \rho) = f(\sigma\tau, \rho)\, \rho\{f(\sigma, \tau)\}.$$

DEFINITION 3.9. If L is a Galois extension of F with Galois group G and f is a factor set, the crossed product algebra $A = (L, G, f)$ is defined as follows:

$$A = \left\{ \sum_{\sigma \in G} u_\sigma l_\sigma \mid l_\sigma \in L \right\}$$

as an L-vector space with basis the symbols $\{u_\sigma\}$. The algebra structure of A is determined by the relations

$$l u_\sigma = u_\sigma \sigma(l), \quad l \in L, \qquad u_\sigma u_\tau = u_{\sigma\tau} f(\sigma, \tau), \quad \sigma, \tau \in G.$$

THEOREM 3.4 [12, Theorem 4.4.1]. *If $A = (L, G, f)$ as in Definition 3.9, A is a central simple F-algebra with splitting field L. Moreover, given any central simple F-algebra B, there exist L, G, f so that, in the Brauer group $\mathrm{B}(F)$, $[B] = [(L, G, f)]$.* ∎

In general, not all central simple algebras are crossed products. This was first established by Amitsur [3].

DEFINITION 3.10. A field F is called fully crossed if every central simple algebra over any finite extension of F is a crossed product.

EXAMPLE 3.4. (a) Any algebraically closed field F is trivially fully crossed since $\mathrm{B}(F) = \{0\}$.

(b) The real number field $\mathbb{R}$ is fully crossed.

(c) Algebraic number fields (i.e., finite extensions of the rational number field) are fully crossed [2, 5].

THEOREM 3.5 [1, Theorems 5.9–5.14]. *Let L be a Galois extension of F with cyclic Galois group $G = \langle\sigma\rangle$ of order $|G| = m$. Then*

$$F^*/N(L^*) \simeq \mathrm{B}(L/F)$$

by

$$aN(L^*) \mapsto [(L, G, f)],$$

where

$$N(b) = \sum_{i=0}^{m-1} \sigma^i(b),$$

$$f(\sigma^i, \sigma^j) = 1, \qquad i + j < m,$$

$$= a, \qquad i + j \geqslant m. \quad \blacksquare$$

THEOREM 3.6 [2, 5]. *Any central simple algebra over an algebraic number field may be represented as a crossed product (L, G, f), where G is cyclic.* ∎

DEFINITION 3.11. The Jacobson radical $\mathrm{J}(A)$ of an F-algebra A is the maximal nilpotent two-sided ideal of A.

EXAMPLE 3.5. (a) If $f(x) = x^n$ in the polynomial algebra $F[x]$, the quotient algebra F_f has Jacobson radical the ideal $\langle x \rangle_f$ generated by the equivalence class of x.

(b) The F-algebra of all upper triangular matrices with entries from F has Jacobson radical the set of all upper triangular matrices with zero along the main diagonal.

THEOREM 3.7 [12, Theorem 1.2.4]. *If A is an F-algebra,*

$$\mathrm{J}\{A/\mathrm{J}(A)\} = \{0\}. \quad \blacksquare$$

That is, the Jacobson radical of the quotient $A/\mathrm{J}(A)$ is trivial.

DEFINITION 3.12. The F-algebra A is called semisimple if $\mathrm{J}(A) = \{0\}$.

THEOREM 3.8 [12, Theorem 2.1.7]. *The F-algebra A is semisimple iff A is a finite Cartesian product of simple F-algebras.* ∎

DEFINITION 3.13. The field F is perfect if every finite extension of F is separable over F.

THEOREM 3.9 [6, Theorem 72.19] (Wedderburn principal theorem). *If A is an algebra over a perfect field F, there is a semisimple F-subalgebra S of A with*

$$S \simeq A/\mathrm{J}(A) \qquad \text{as} \quad F\text{-algebras}$$

and

$$A = S \oplus \mathrm{J}(A) \qquad \text{as} \quad F\text{-vector spaces.} \quad \blacksquare$$

4. Multiplicative Complexity of Central Simple Algebras over Algebraic Number Fields

This section is a study of the multiplicative complexity of a central simple algebra over an algebraic number field. We first show that any two n-dimensional central simple algebras over an algebraic number field have the same order of complexity. Specifically, we prove that if A and B are central simple algebras over a number field F with $(A:F) = (B:F)$, then $4\pi(A) \geqslant \pi(B) \geqslant \frac{1}{4}\pi(A)$ (Theorem 4.2). In the second portion of this section, we specialize our attention to the complexity of a central simple algebra A of dimension p^2, p a prime, over an algebraic number field F containing all pth roots of unity. In this setting we prove (Theorem 4.5) that

$$4\pi((F, \gamma)) \leqslant \pi(A) \leqslant (\tfrac{1}{4})\,\pi((F, \gamma))$$

for some pth root of unity γ, where the twisted truncated polynomial algebra (F, γ) is defined as the quotient of the free F-algebra $F[\![X, Y]\!]$ on the noncommuting indeterminates X, Y modulo the ideal generated by the relations

$$XY = \gamma YX \qquad X^p = 0 = Y^p.$$

THEOREM 4.1. *Let L be a Galois extension of an infinite field F with cyclic Galois group G. Then, for any crossed products (L, G, f) and (L, G, g),*

$$2\pi((L, G, f)) \geqslant \pi((L, G, g)) \geqslant \tfrac{1}{2}\pi((L, G, f)).$$

Proof. If (L, G, h) is an arbitrary crossed product and $G = \langle\sigma\rangle$ of order m, then by [1, Theorem 5.9] we may assume

$$\begin{aligned} h(\sigma^i, \sigma^j) &= 1, \qquad i + j < m, \\ &= c, \qquad i + j \geqslant m, \end{aligned}$$

for some c in F^*. Since $G = \langle\sigma\rangle$, we use the symbols $\underline{\sigma}^i$ instead of $u_{\sigma i}$ (see Definition 3.9) to denote the L-basis of $(L, G, h) \equiv (L, G, c)$.

Then, for $x = \sum_{i=0}^{m-1} \underline{\sigma}^i x_i$, $y = \sum_{j=0}^{m-1} \underline{\sigma}^j y_j$ in (L, G, c),

$$\begin{aligned} x \cdot y &= \sum_{i,j=0}^{m-1} \underline{\sigma}^{i+j} \sigma^j(x_i)\, y_j h(i, j) \\ &= \sum_{i,l=0}^{m-1} \underline{\sigma}^l \sigma^{l-i}(x_i)\, y_{l-i} h(i, l-i), \\ &= \sum_{l=0}^{m-1} \underline{\sigma}^l \left\{ \sum_{i=0}^{l} \sigma^{l-i}(x_i)\, y_{l-i} + c \sum_{i=l+1}^{m-1} \sigma^{l-i}(x_i)\, y_{l-i} \right\}. \end{aligned}$$

Since F is infinite, we may choose $c_1 \neq c$ in F^* with $cN(L^*) = c_1 N(L^*)$, or equivalently, $(L, G, c) \simeq (L, G, c_1)$. Computing the product $(x_0, \ldots, x_{m-1})^*$

$(y_0,\ldots, y_{m-1})$ in each of these two isomorphic algebras and then subtracting corresponding coefficients of $\underline{\sigma}^l$ allows one to compute, for $l = 0,\ldots, m-1$,

$$\sum_{i=0}^{l} \sigma^{l-i}(x_i)\, y_{l-i}$$

and

$$\sum_{i=l+1}^{m-1} \sigma^{l-i}(x_i)\, y_{l-i}$$

with $2\pi((L, G, c)) = 2\pi((L, G, c_1))$ multiplications. Since (L, G, h) was an arbitrary crossed product, it follows that

$$2\pi((L, G, f)) \geqslant \pi((L, G, g)) \geqslant \tfrac{1}{2}\pi((L, G, f))$$

for any factor sets f and g. ∎

For the remainder of this section, we shall assume that the base field F is an algebraic number field.

THEOREM 4.2. *Let A and B be two central simple algebras over the algebraic number field F with $(A:F) = (B:F) = n = m^2$. Then*

$$4\pi(A) \geqslant \pi(B) \geqslant \tfrac{1}{4}\pi(A).$$

Proof. By Theorem 3.6, A and B have cyclic crossed product representations, say, $A = (L, G, f)$ and $B = (L_1, G_1, f_1)$. Note that $M(m, F) = (L, G, f) = (L_1, G_1, f_1)$. Thus, by Theorem 4.1,

$$2\pi(M(m, F)) \geqslant \pi(A) \geqslant \tfrac{1}{2}\pi(M(m, F))$$

and

$$2\pi(M(m, F)) \geqslant \pi(B) \geqslant \tfrac{1}{2}\pi(M(m, F)).$$

Hence

$$4\pi(A) \geqslant \pi(B) \geqslant \tfrac{1}{4}\pi(A). \quad ∎$$

Therefore, if we are just interested in the multiplicative complexity of a central simple algebra over an algebraic number field F to within a constant factor, we need only consider the trivial central simple algebras $M(m, F)$ for m any positive integer. Recall that, if $m = \prod_{i=1}^{l} p_i^{n_i}$ is the prime factorization of m,

$$M(m, F) \simeq \bigotimes_{i=1}^{l} \left[\bigotimes_{j=1}^{n_i} M(p_i, F) \right].$$

Hence to obtain upper bounds on the complexity of a central simple algebra over an algebraic number field, it is sufficient to study the complexity of $M(p, F)$ for a prime p.

In order to explore the multiplicative complexity of $M(p, F)$ we make one final constraint of F. We assume that F contains all the pth roots of unity. In addition, we shall need the following theorem from field theory:

THEOREM 4.3. *Let F be a field containing all the pth roots of unity for a prime p not equal to the characteristic of F. Suppose L is a Galois extension of F of degree p with cyclic Galois group $G = \langle\sigma\rangle$. Then L is generated (as a field) over F by the pth root β of an element of F with $\sigma^i(\beta) = \gamma^{-i}\beta$ for some pth root of unity γ.*

Proof. Choose α in $L - F$. Then $L = F(\alpha)$ since $(L : F) = p$ is a prime. Define the Lagrange resolvent (relative to α) for a pth root of unity γ to be

$$(\alpha, \gamma) = \alpha + \sigma(\alpha)\gamma + \cdots + \sigma^{p-1}(\alpha)\gamma^{p-1}.$$

Then

$$\sigma\{(\alpha, \gamma)\} = \sigma(\alpha) + \sigma^2(\alpha)\gamma + \cdots + \alpha\gamma^{p-1}\sigma\{(\alpha, \gamma)\} = \gamma^{-1}(\alpha, \gamma).$$

Hence

$$\sigma\{(\alpha, \gamma)^p\} = \{\sigma(\alpha, \gamma)\}^p = \{\gamma^{-1}(\alpha, \gamma)\}^p = (\alpha, \gamma)^p$$

so $(\alpha, \gamma)^p$ is in F. If we can show there is a pth root of unity γ_0 for which (α, γ_0) is not in F, we shall be done with $\beta = (\alpha, \gamma_0)$. Note, however, that

$$\sum_{\gamma} (\alpha, \gamma) = p\alpha \neq 0,$$

since $\sum_{i=0}^{p-1} \gamma^i = 0$. Then, because $\alpha \notin F$, all of the (α, γ)'s cannot be in F.

In addition,

$$\sigma^i\{(\alpha, \gamma)\} = \sigma^{i-1}\{\gamma^{-1}(\alpha, \gamma)\} = \gamma^{-1}\sigma^{i-1}\{(\alpha, \gamma)\} = \gamma^{-i}(\alpha, \gamma),$$

by the definition of the Lagrange resolvent. ∎

Now we are prepared to consider the multiplicative complexity of a cyclic crossed product (L, G, a), where

L is a Galois extension of F of degree p,

$G = \langle\sigma\rangle$,

F contains all pth roots of unity,

$L = F(\beta)$ for $\beta \in L$ with $\beta^p = b \in F$,

$\sigma^i(\beta) = \gamma^{-i}\beta$ for some pth root of unity γ for all i.

Let

$$x = \sum_{i=0}^{p-1} \underline{\sigma}^i x_i, \qquad y = \sum_{j=0}^{p-1} \underline{\sigma}^j y_j,$$

be in $(L, G, a) = (L, G, f)$ with $x_i, y_j \in L$. Then

$$\begin{aligned} x \cdot y &= \sum_{i,j=0}^{p-1} \underline{\sigma}^{i+j} \sigma^j(x_i)\, y_j f(i, j), \\ x \cdot y &= \sum_{j,l=0}^{p-1} \underline{\sigma}^l \sigma^j(x_{l-j})\, y_j f(l-j, j). \end{aligned} \tag{1}$$

Now suppose that

$$x_{l-j} = \sum_{i=0}^{p-1} x_{l-j,i} \beta^i, \qquad y_j = \sum_{m=0}^{p-1} y_{j,m} \beta^m,$$

with $x_{l-j,i}, y_{j,m} \in F$. Then we may rewrite Eq. (1) as

$$\begin{aligned} x \cdot y &= \sum_{j,l=0}^{p-1} \underline{\sigma}^l \left\{ \left[\sum_{i=0}^{p-1} x_{l-j,i} \gamma^{-ji} \beta^i \right] \left[\sum_{m=0}^{p-1} y_{j,m} \beta^m \right] f(l-j, j) \right\} \\ &= \sum_{l=0}^{p-1} \underline{\sigma}^l \left\{ \sum_{j=0}^{p-1} \left[\sum_{i=0}^{p-1} x_{l-j,i} \gamma^{-ji} \beta^i \right] \left[\sum_{m=0}^{p-1} y_{j,m} \beta^m \right] f(l-j, j) \right\} \\ &= \sum_{l=0}^{p-1} \underline{\sigma}^l \left\{ \sum_{j=0}^{p-1} \left[\sum_{s=0}^{p-1} \left[\sum_{r=0}^{s} x_{l-j,r} \gamma^{-jr} y_{j,s-r} \right. \right. \right. \\ &\quad \left. \left. \left. + b \sum_{r=s+1}^{p-1} x_{l-j,r} \gamma^{-jr} y_{j,p+s-r} \right] \beta^s \right] f(l-j, j) \right\} \\ &= \sum_{s,l=0}^{p-1} \underline{\sigma}^l \beta^s \left\{ \sum_{j=0}^{l} \sum_{r=0}^{s} x_{l-j,r} \gamma^{-jr} y_{j,s-r} \right. \\ &\quad + b \sum_{j=0}^{l} \sum_{r=s+1}^{p-1} x_{l-j,r} \gamma^{-jr} y_{j,s-r} \\ &\quad + a \sum_{j=l+1}^{p-1} \sum_{r=0}^{s} x_{l-j,r} \gamma^{-jr} y_{j,s-r} \\ &\quad \left. + ab \sum_{j=l+1}^{p-1} \sum_{r=s+1}^{p-1} x_{l-j,r} \gamma^{-jr} y_{j,p+s-r} \right\} \\ &\equiv \sum_{s,l=0}^{p-1} \underline{\sigma} \beta^s \{A_{l,s} + bB_{l,s} + aC_{l,s} + abD_{l,s}\}. \end{aligned} \tag{2}$$

This F-algebra $(L, G, a) = (L, G, f)$ can thus also be described in the following manner. Let X and Y be noncommuting indeterminates over F, and form the free F-algebra $F[\![X, Y]\!]$ on the symbols X and Y. For any a, b in F and pth root of unity γ, denote the ideal of $F[\![X, Y]\!]$ generated by the relations

$$XY = \gamma YX, \qquad X^p = b, \qquad Y^p = a$$

by $I(p, \gamma, a, b)$. Then the quotient algebra

$$(p, \gamma, a, b) \equiv F[\![X, Y]\!]/I(p, \gamma, a, b)$$

is (L, G, a) as given.

Referring to Eq. (2), it is clear that computing $\{A_{j,s}\}_{j,s=0}^{p-1}$ is the same as computing the product in $(p, \gamma, 0, 0) \equiv (F, \gamma)$. If we introduce the changes in notation

$$x_{j-i,r} = \bar{x}_{j-i,p-1-r}, \qquad y_{i,s-r} = \bar{y}_{i,p-1(s-r)},$$
$$R = p - 1 - r, \qquad S = p - 2 - s,$$

computing $\{B_{j,s}\}_{j,s=0}^{p-1}$ is equivalent to computing $\{\bar{B}_{j,S}\}_{j=0,S=0}^{p-1,p-2}$, where

$$\bar{B}_{j,S} = \sum_{i=0}^{j} \sum_{R=0}^{S} \bar{x}_{j-i,R} \gamma^{-i(p-1-R)} y_{i,S-R}.$$

Therefore the complexity of computing $\{B_{j,s}\}_{j,s=0}^{p-1}$ is less than or equal to $\pi((p, \gamma, 0, 0))$. Similarly, the complexity of computing $\{C_{j,s}\}_{j,s=0}^{p-1}$ or $\{D_{j,s}\}_{j,s=0}^{p-1}$ is bounded above by $\pi((p, \gamma, 0, 0))$. Hence, for any a, b in F,

$$\pi((p, \gamma, a, b)) \leqslant 4\pi((p, \gamma, 0, 0)).$$

By generating four equations in the unknowns $A_{j,s}$, $B_{j,s}$, $C_{j,s}$, and $D_{j,s}$ by computing the product in four isomorphic copies of the algebra (p, γ, a, b) it may thus be seen that:

THEOREM 4.4. *For all a, b, c, d in F,*

$$4\pi((p, \gamma, a, b)) \geqslant \pi((p, \gamma, c, d)) \geqslant \tfrac{1}{4}\pi((p, \gamma, a, b)). \quad \blacksquare$$

Combining Theorems 3.6 and 4.4, one immediately obtains

THEOREM 4.5. *Let F be an algebraic number field containing all pth roots of unity for a prime p and let L be a degree p Galois extension of F with $L = F((\alpha, \gamma))$ for the Lagrange resolvent (α, γ). Suppose that A is a central simple F-algebra of dimension p^2 with splitting field L. Then*

$$\tfrac{1}{4}\pi((F, \gamma)) \leqslant \pi(A) \leqslant 4\pi((F, \gamma)). \quad \blacksquare$$

5. Multiplicative Complexity and Nilpotency

The purpose of this section is to prove the following theorem:

Let F be a fully crossed perfect field and A be an n-dimensional F-algebra with Jacobson radical $J(A)$ such that $J(A)^2 = \{0\}$. Then $\pi(A) = O(n^{1.5})$.

We shall prove this theorem by first treating the case, where A is a central simple F-algebra, and then gradually reducing the constraints on A.

THEOREM 5.1. *Let F be a fully crossed field and A be a central simple F-algebra of dimension n. Then $\pi(A) = O(n^{1.5})$.*

Proof. Since F is fully crossed, there is a Galois extension L of F with Galois group G of order $|G| = \sqrt{n}$ and a factor set f such that $A = (L, G, f)$. If

$$x = \sum_{\sigma \in G} u_\sigma x_\sigma, \qquad y = \sum_{\tau \in G} u_\tau y_\tau$$

in (L, G, f),

$$x \cdot y = \left(\sum_{\sigma \in G} u_\sigma x_\sigma \right) \left(\sum_{\tau \in G} u_\tau y_\tau \right) = \sum_{\sigma, \tau \in G} u_{\sigma\tau} \tau(x_\sigma) y_\tau f(\sigma, \tau).$$

Thus

$$\pi(A) \leqslant 2|G|^2(\pi(L)) = 2|G|^2(2|G| - 1) = 4n^{1.5} - 2n. \quad \blacksquare$$

THEOREM 5.2. *Let A be a simple n-dimensional algebra over the fully crossed field F. Then $\pi(A) = O(n^{1.5})$.*

Proof. Let $r = (A : Z(A))$, $s = (Z(A) : F)$ so that $n = rs$. Then

$$\pi(A) \leqslant \pi_{Z(A)}(A)\, \pi(Z(A)).$$

Since $Z(A)$ is a field and A is a central simple $Z(A)$-algebra,

$$\pi(A) \leqslant (4r^{1.5} - 2r)(2s - 1).$$

Hence

$$\pi(A) = O((rs)^{1.5}) = O(n^{1.5}). \quad \blacksquare$$

THEOREM 5.3. *Let A be a semisimple n-dimensional algebra over the fully crossed field F. Then $\pi(A) = O(n^{1.5})$.*

Proof. Since A is semisimple, there exist simple F-algebras $A_1, \ldots, A_s$ with

$$A \simeq \prod_{i=1}^{s} A_i.$$

Thus

$$\pi(A) \leqslant \sum_{i=1}^{s} \pi(A_i)$$

implies

$$\pi(A) = O(n^{1.5}). \quad \blacksquare$$

For the remainder of this section, we assume that F is perfect. Then by the Wedderburn principal theorem A may be written as

$$A = B \oplus \mathrm{J}(A),$$

where B is a semisimple subalgebra and $\mathrm{J}(A)$ is the Jacobson radical of A. Since B is semisimple, there are simple subalgebras $B_1,\ldots, B_s$ with $B = \prod_{i=1}^{s} B_i$. Hence $1 \in B$ may be written as $1 = \sum_{i=1}^{s} e_i$ with $e_i \in B_i$ orthogonal idempotents. Then

$$\mathrm{J}(A) = \mathrm{J}(A) \cdot 1 = \prod_{i=1}^{s} \mathrm{J}(A)e_i = 1 \cdot \mathrm{J}(A) = \prod_{i=1}^{s} e_i \mathrm{J}(A).$$

If $\mathrm{J}(A)^2 = \{0\}$, $\mathrm{J}(A)$ is a left and right module over the ring B.

DEFINITION 5.1. Let R be an F-algebra, M a left R-module, and N a right R-module. Define $\pi(R, M)$ to be the (bilinear) multiplicative complexity of computing $x \cdot m$ for $x \in R$, $m \in M$. Similarly $\pi(N, R)$ is the (bilinear) multiplicative complexity of computing $n \cdot x$ for $x \in R$, $n \in N$. Note that $\pi(R, R) = \pi(R)$.

The subaddivity of the complexity of a Cartesian product immediately yields

THEOREM 5.4. *Let A be an algebra over a perfect field F with $\mathrm{J}(A)^2 = \{0\}$ and $A = B \oplus \mathrm{J}(A)$, $B = \prod_{i=1}^{s} B_i$, B_i simple, $1 = \sum_{i=1}^{s} e_i$, where $e_1,\ldots, e_s$ are orthogonal idempotents*:

$$\pi(A) \leqslant \sum_{i=1}^{s} \{\pi(B_i) + \pi(B_i, \mathrm{J}(A)e_i) + \pi(e_i\mathrm{J}(A), B_i)\}. \quad \blacksquare \tag{3}$$

To obtain an upper bound on $\pi(A)$, it is thus sufficient to determine upper bounds for the last two terms of Eq. (5), $\pi(B_i, \mathrm{J}(A)e_i)$, and $\pi(e_i\mathrm{J}(A), B_i)$. This is accomplished via Lemma 5.1, which shows that these multiplication problems are both matrix multiplication problems.

LEMMA 5.1. *With notation as in Theorem* 5.4, *$\mathrm{J}(A)e_i$ is isomorphic as a left B_i-module to a direct product of columns of $B_i \simeq M(m_i, D_i)$.* Also, *$e_i\mathrm{J}(A)$ is isomorphic as a right B_i-module to a direct product of rows of B_i.*

Proof. The lemma follows directly from the structure theory of modules over semisimple rings [12, Sect. 4.3]. ∎

Hence, combining Theorems 5.3 and 5.4 with Lemma 5.1, we have

THEOREM 5.5. *Let A be an n-dimensional algebra over the fully crossed perfect field F. Then, if* $\mathrm{J}(A)^2 = \{0\}$,

$$\pi(A) = O(n^{1.5}). \quad \blacksquare$$

Hence any algebra over a fully crossed field of characteristic zero with hard-to-compute multiplication (see Fiduccia [9, 10]) must have an index of nilpotency of its Jacobson radical greater than two.

ACKNOWLEDGMENT

I would like to thank C. M. Fiduccia for stimulating discussions and introducing me to the multiplicative complexity literature.

REFERENCES

1. A. A. ALBERT, "Structure of Algebras," American Mathematical Society Colloq. Publ. XXIV, Providence, R. I., 1939.
2. A. A. ALBERT AND H. HASSE, A determination of all normal division algebras over an algebraic number field, *Trans. Amer. Math. Soc.* **34** (1932), 722–726.
3. S. A. AMITSUR, On central division algebras, *Israel J. Math.* **12** (1972), 408–420.
4. D. BINI AND M. CAPOVANI, Lower bounds of the complexity of linear algebras, *Inform. Process. Lett.* **9** (1979), 46–47.
5. R. BRAUER, H. HASSE, AND E. NOETHER, Beweis eines Hauptsatzes in der Theorie der Algebren, *J. Reine Angew. Math.* **167** (1932), 399–404.
6. C. CURTIS AND I. REINER, "Representation Theory of Finite Groups and Associative Algebras," Wiley–Interscience, New York, 1962.
7. D. DOBKIN, "On the Arithmetic Complexity of a Class of Arithmetic Computations," Res. Rep. No. 23, Yale Univ. Press, New Haven, Conn., 1973.
8. C. M. FIDUCCIA AND Y. ZALCSTEIN, Algebras having linear multiplicative complexities, *J. Assoc. Comput.* **24** (1977), 311–331.
9. C. M. FIDUCCIA, Hard-to-compute bilinear forms, *in* "Proc. 1978 Conf. Inf. Sciences and Systems," pp. 40–45, Johns Hopkins Press, Baltimore.
10. C. M. FIDUCCIA, "Real and Complex Tensors of Near Maximal Rank," Gen. Electr. Research & Development Center, Report No. 69CRD051, 1978.
11. H. F. DEGROOTE, On the complexity of quaternion multiplication, *Inform. Process. Lett.* **3** (1975), 177–179.
12. I. HERSTEIN, "Noncommutative Rings," Carus Mathematical Monograph Series, No. 15, Mathematical Association of America, Washington, D. C., 1968.
13. T. D. HOWELL, "Tensor Rank and the Complexity of Bilinear Forms," Ph. D. Dissertation, Cornell University, Ithaca, New York, 1976.
14. V. STRASSEN, Gaussian elimination is not optimal, *Numer. Math.* **13** (1969), 354–356.
15. S. WINOGRAD, On multiplication of 2×2 matrices, *Linear Algebra Appl.* **4** (1971), 381–388.